NBS TECHNICAL NOTE 809

Government Looks at

PRIVACY and SECURITY in COMPUTER SYSTEMS

U.S.
PARTMENT
OF
OMMERCE
National
Bureau
of
Standards

NATIONAL BUREAU OF STANDARDS

The National Bureau of Standards [1] was established by an act of Congress March 3, 1901. The Bureau's overall goal is to strengthen and advance the Nation's science and technology and facilitate their effective application for public benefit. To this end, the Bureau conducts research and provides: (1) a basis for the Nation's physical measurement system, (2) scientific and technological services for industry and government, (3) a technical basis for equity in trade, and (4) technical services to promote public safety. The Bureau consists of the Institute for Basic Standards, the Institute for Materials Research, the Institute for Applied Technology, the Institute for Computer Sciences and Technology, and the Office for Information Programs.

THE INSTITUTE FOR BASIC STANDARDS provides the central basis within the United States of a complete and consistent system of physical measurement; coordinates that system with measurement systems of other nations; and furnishes essential services leading to accurate and uniform physical measurements throughout the Nation's scientific community, industry, and commerce. The Institute consists of a Center for Radiation Research, an Office of Measurement Services and the following divisions:

Applied Mathematics — Electricity — Mechanics — Heat — Optical Physics — Nuclear Sciences [2] — Applied Radiation [2] — Quantum Electronics [3] — Electromagnetics [3] — Time and Frequency [3] — Laboratory Astrophysics [3] — Cryogenics [3].

THE INSTITUTE FOR MATERIALS RESEARCH conducts materials research leading to improved methods of measurement, standards, and data on the properties of well-characterized materials needed by industry, commerce, educational institutions, and Government; provides advisory and research services to other Government agencies; and develops, produces, and distributes standard reference materials. The Institute consists of the Office of Standard Reference Materials and the following divisions:

Analytical Chemistry — Polymers — Metallurgy — Inorganic Materials — Reactor Radiation — Physical Chemistry.

THE INSTITUTE FOR APPLIED TECHNOLOGY provides technical services to promote the use of available technology and to facilitate technological innovation in industry and Government; cooperates with public and private organizations leading to the development of technological standards (including mandatory safety standards), codes and methods of test; and provides technical advice and services to Government agencies upon request. The Institute consists of a Center for Building Technology and the following divisions and offices:

Engineering and Product Standards — Weights and Measures — Invention and Innovation — Product Evaluation Technology — Electronic Technology — Technical Analysis — Measurement Engineering — Structures, Materials, and Life Safety [4] — Building Environment [4] — Technical Evaluation and Application [4] — Fire Technology.

THE INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY conducts research and provides technical services designed to aid Government agencies in improving cost effectiveness in the conduct of their programs through the selection, acquisition, and effective utilization of automatic data processing equipment; and serves as the principal focus within the executive branch for the development of Federal standards for automatic data processing equipment, techniques, and computer languages. The Institute consists of the following divisions:

Computer Services — Systems and Software — Computer Systems Engineering — Information Technology.

THE OFFICE FOR INFORMATION PROGRAMS promotes optimum dissemination and accessibility of scientific information generated within NBS and other agencies of the Federal Government; promotes the development of the National Standard Reference Data System and a system of information analysis centers dealing with the broader aspects of the National Measurement System; provides appropriate services to ensure that the NBS staff has optimum accessibility to the scientific information of the world. The Office consists of the following organizational units:

Office of Standard Reference Data — Office of Information Activities — Office of Technical Publications — Library — Office of International Relations.

---

[1] Headquarters and Laboratories at Gaithersburg, Maryland, unless otherwise noted; mailing address Washington, D.C. 20234.
[2] Part of the Center for Radiation Research.
[3] Located at Boulder, Colorado 80302.
[4] Part of the Center for Building Technology.

Government Looks at
PRIVACY and SECURITY in COMPUTER SYSTEMS

A Summary of a Conference
Held at the National Bureau of Standards,
Gaithersburg, Maryland, November 19-20, 1973

Clark R. Renninger

and

Dennis K. Branstad, Editors

Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D.C. 20234

U.S. DEPARTMENT OF COMMERCE, Frederick B. Dent, *Secretary*
NATIONAL BUREAU OF STANDARDS, Richard W. Roberts, *Director*

Issued February 1974

National Bureau of Standards Technical Note 809

Nat. Bur. Stand. (U.S.), Tech. Note 809, 47 pages (Feb. 1974)

CODEN: NBTNAE

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1974

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402
(Order by SD Catalog No. C13.46:809). Price 85 cents.

FOREWORD

Any potential confrontation between society and technology over problems of individual privacy and data confidentiality can be defused by understanding and action. The Conference on Privacy and Computer Security has contributed to both by providing an initial statement of governmental needs and problems and suggesting a broad range of activities for satisfying them. We hope this Conference report will serve as the foundation for a continuing dialogue among the government, automation industries, service industries, and the consumer which will lead to a refinement of this statement and the assumption of relevant responsibilities for achieving effective solutions.

Ruth M. Davis, Ph.D.
Director, Institute for
Computer Sciences and Technology
National Bureau of Standards
U.S. Department of Commerce

EXECUTIVE SUMMARY

A two-day conference on Privacy and Security in Computer Systems was sponsored by and held at the National Bureau of Standards on November 19-20, 1973. Five hundred and ten people from government, the computer industry, and various public interest groups met to hear presentations of the needs and problems that confront governmental agencies in safeguarding individual privacy and protecting confidential data from loss or misuse.

Lawmakers at Federal, State and local levels of government are increasingly aware of the public's concern over computer-based recordkeeping and its implications for personal privacy. This concern has arisen partly out of fear of the impersonal super-efficient image that computers present and partly out of a reasoned concern over the expansion of governmental recordkeeping activities which computers make possible. Lawmakers are responding to this concern by proposing and enacting laws that are intended to specifically safeguard the rights and interests of individuals by prescribing the circumstances and the manner in which personal data can be collected, used and disseminated.

These legislative actions, if taken unilaterally, present the prospect of potentially conflicting requirements being imposed upon those charged with their implementation. Further, the technological capability needed to assure compliance with these requirements is not generally available. Compounding these problems are increased public pressures to operate governments economically. These pressures foreclose the simplistic solution of using dedicated computers to process confidential data, yet the computer systems presently available for resource sharing provide few techniques for controlling access to confidential data. These interrelated considerations strongly suggest that all of the legislative, technological and managerial solutions that can be brought to bear upon the problems of privacy and security must be effectively integrated so that a proper balance of needs and values in relation to costs can be achieved.

The assignment and acceptance of responsibilities for accomplishing this objective requires a recognition of the separable but interrelated components of the privacy and computer security problems. These may be identified as:

- Protection of the privacy of the individual: a responsibility of the legislative and judiciary branches of government.

- Providing guidelines to assure information management is in compliance with legislative and judicial requirements for privacy: a responsibility of government, management, and industry.

- Development and application of the needed automation and information management technologies and products: a responsibility of industry and the government.

° Assessment and assignment of the costs of Security in Automation: a responsibility of the government, industry and the public.

° Management of information in automated record-keeping systems: a responsibility of management and information management technologists.

While the solutions for safeguarding privacy are to be found in legislative or regulatory sources, solutions for protecting confidential data are found in physical security measures and in the technological safeguards and procedures which permit controlled accessibility to the systems and data.

The broad scope of controlled accessibility precludes simple solutions. It embraces the use of specialized hardware and software with built-in protective features, mechanisms for authorizing access to systems and data, techniques for uniquely identifying individuals who are authorized to gain access, cryptographic devices and encryption algorithms to protect data during transmission among systems, and auditing or monitoring techniques for measuring system events of security interest.

While various techniques for access control exist, there are few guidelines for the application of these techniques. Lacking such guidelines, system users apply protection controls that are either inadequate or excessively costly for the degree of protection they require. The importance of considering the cost of applying security measures cannot be over-emphasized, since security is always a cost vs. effectiveness trade-off. A highly important extension of this managerial concern is the question of how much the public will be willing to pay for the protection of individual privacy and how the incremental cost for security is to be allocated among government, industry and the public.

Major needs for alleviating the problems of privacy, data confidentiality and computer security were identified on an initial basis. A realistic approach for addressing these needs could consist of parallel and coordinated efforts directed toward:

° Achieving a national coherence among laws defining the privacy rights of individuals and the basic information practices to be followed in protecting these rights.

° Establishing uniform management and technical procedures for effectively applying security measures. Important needs are techniques for assessing risks, determining threats and threat sources, evaluating alternative security measures, auditing the effectiveness of existing measures and physical security.

° Innovative applications of existing technology to enhance security effectiveness. Specific needs which are susceptible to solution in this way include the retrofitting of existing systems to satisfy new security requirements and the use of

encryption techniques in civilian applications for protecting data during transmission.

° Research and development of new mechanisms and techniques where significant needs cannot be met satisfactorily by existing technology. Among the needs requiring this type of effort are self-protected computer systems which have the internal ability to enforce the access controls necessary for the prescribed level of security. Other needs include techniques for positively and uniquely identifying individuals who have authorization for access to the system and data and the development of secure network models for evaluating alternative network designs.

° A study of the costs of data confidentiiality and security to build an understanding useful in making public choices about degrees of privacy desired by individuals and for allocating costs among the public, industry and government.

It is hoped that the Conference will stimulate the computer industry and other interested parties to propose specific approaches and solutions to the needs and problems outlined and will promote new initiatives for protecting data confidentiality in computer-based records systems.

A second Conference is planned for March 4-5, 1974, which will provide an opportunity for the presentation of proposed technological and regulatory solutions to the computer security needs and problems identified in this Conference.

TABLE OF CONTENTS

Government Looks At Privacy and Security in Computer Systems

Summary of a Conference held at the National Bureau of Standards, Gaithersburg, Maryland

November 19-20, 1973

Clark R. Renninger and Dennis K. Branstad, Editors

This publication summarizes the proceedings of a conference held for the purpose of highlighting the needs and problems of Federal, State, and local governments in safeguarding individual privacy and protecting confidential data contained in computer systems from loss or misuse. The Conference was held at the National Bureau of Standards on November 19-20, 1973.

The origin of governmental problems is discussed in the context of the public's concern for privacy arising out of computer-based recordkeeping, the diverse legislative actions now being taken to safeguard privacy, the threats to the security of computer-based information systems and the technological problems associated with protecting against such threats. Useful distinctions are drawn between privacy, confidentiality and security to clarify the issues and allocate responsiblities for solving the problem among lawmakers, technologists and management.

Major needs are described. These include the need for cohesive Federal, State and local legislation; technological guidelines and standards for assuring uniform compliance with legislative requirements; management guidelines for identifying and evaluating threats to security; and improved technological mechanisms for controlling access to computer systems and networks. Cost implications of providing security measures are discussed.

Key words: Computer systems, privacy and security; confidentiality; privacy; security.

I. Introduction

1.1. Purpose of the Conference

This paper is a summary of a two-day Conference on Privacy and Security in Computer Systems, held on November 19-20, 1973, and sponsored by the Institute for Computer Sciences and Technology of the National Bureau of Standards.

In his introductory remarks, Dr. Richard W. Roberts, Director, NBS, indicated that the Conference was attended by 510 people: 375 of them from Federal, State and local governments, and 135 from the private sector. These attendees represented 7 Congressional offices, 46 Federal agencies, 30 States, 7 local governments, 34 computer companies and 41 professional associations, universities and public interest groups.

The stated purpose of the conference was to:

531-849 O - 74 - 2

"Identify initial requirements and issues that confront governmental organizations in safeguarding individual privacy, data confidentiality and computer security.

"Communicate this information to groups in the public and private sector in order to mobilize and orient efforts that can respond to recognized needs.

"Establish a foundation for a second conference to be held on March 4-5, 1974, which will provide the opportunity for the presentation of proposed technological or regulatory solutions to the computer security needs and problems identified in this Conference."

1.2. Organization of the Summary

This summary identifies the principal themes of the various presentations and organizes them to:

A. Identify the origins of the problems encountered by Federal, State and local governmental bodies in attempting to meet their responsibilities in safeguarding information needed to perform governmental functions.

B. Describe the milieu in which they operate.

C. Describe the problems as seen by Federal, State and local governments.

D. Discuss the issues of costs.

E. Present suggestions for action.

The summary is an integration of the papers and presentations of the Conference. In all cases, it is believed that the intent of the speakers has been preserved.

1.3. Appendices

A. The Conference Program

B. References to source materials cited at the Conference

C. A preview of the March 4-5, 1974, conference

II. Where the Problem Arises

2.1. Public Interest

In the keynote address, John K. Tabor, Under Secretary of Commerce, noted a number of factors that are creating pressure for solutions to the problems of providing protection to confidential or valuable data against misuse or loss. He cited the general expansion of government and private information gathering and recordkeeping to support the needs of

society as a phenomenon of recent American life. The capability to manage large recordkeeping activities and derive useful data is made possible and even accelerated through use of computers. He noted that linking computers through telecommunications multiplies the capability to exchange and share the results of information-collecting activities while at the same time compounding the protection problem. Under Secretary Tabor called for soundly designed safeguards to protect the confidentiality of data collected in support of expanded services and programs at all levels of government.

Congressman Jack Brooks, Chairman of the Government Activities Subcommittee of the House Committee on Government Operations, noted that control over dissemination of such information involves two concepts: privacy, or who should have access to what information for what purposes; and data security, which prevents unauthorized access to the data and also protects its integrity.

In discussing the large number of data banks involving personal data that already exist, Congressman Brooks indicated that 7500 data banks were counted in the Federal Government alone; he further indicated that he believed the count was "low." The number of non-Federal data banks involving personal information is unknown although it was indicated that the State of California has between 8,000 - 10,000 data bases of which approximately 45% (3,600 - 4,500) involve personal data. While these figures represent only two very isolated data points, it is evident that the number of Federal, State and local government data files containing personal data is very large indeed. Coupled with the large or even larger number of files containing personal data to be found in the private sector (e.g., insurance companies, credit card plans, mailing lists, school records, etc.), this represents a very large pool of information that is being actively collected and maintained.

Along with the intensified recordkeeping activities of governmental units has come an increased awareness of the part of the public that such activities are going on, and with this awareness there is an increased sensitivity about individuality and personal rights. It would be stretching facts to suggest that the rise of awareness and feeling of potential threat to one's individuality comes from abuses in the collection and use of data by governmental units. Rather, it would seem that such awareness comes about from a variety of factors present in an increasingly complex society. Regardless, the public's desire for privacy is quite real and has created a conflict between the interests and rights of an individual and the interests and rights of government (and private) institutions. As David B. H. Martin, Special Assistant to the Secretary, HEW, pointed out, this conflict of interests raises the public policy questions that require legislative and regulatory solutions.

Congressman Brooks pointed out that no legislative action can be effective without the corresponding technological advances to support legislative efforts. He said, "The directives of Congress and State legislatures as to constitutional and social restrictions to protect the

rights of individuals will be of little consequence if the data itself is readily available to ill-willed persons using surreptitious or unlawful means."

It is clear that legislators are concerned about the question of rights of individual privacy. They are willing to support legislation that defines these rights and attempts to strike a harmonious balance between the rights of individuals and the rights of society as a whole acting through various institutions and agencies of government.

Dr. Alan Westin, Professor of Public Law and Government, Columbia University, in an interesting review of the international aspects of the privacy question, identified three phases of awareness and action:

a) Early Warning Phase - the crying of public alarm and rising public awareness of the conflict between organizational efficiency and privacy.

b) Study Phase - commissioning of studies to identify the problem.

c) Regulatory Phase - the development of administrative, legal and regulatory safeguards for privacy.

He indicated that most of the Western industrialized nations have passed beyond the initial phase and have moved into the Study and Regulatory Phases, while at the same time the issue is just being recognized in nations with different cultural backgrounds, such as Japan.

In commenting on some 7 - 10 studies performed in a variety of countries, he noted their remarkable similarity, taking into account the differences in terms of reference and cultures. The more significant common findings included:

a) Computer technology increases the efficiency of recordkeeping.

b) There is significant fear (of loss of privacy) on the part of the public.

c) None of the studies could document specific episodes where automated record-keeping created new loss of personal liberties. (Any abuses that were uncovered had existed in pre-automation manual record-keeping times.)

d) Use of computers intensifies problems (of policy, etc.) that existed in manual systems.

e) All of the reports recommended protective measures to protect individual rights.

Those countries having advanced to the regulatory phase appear to be evolving three patterns of approach to regulation. These were summarized as administrative self-regulation (the British approach), omnibus licensing and regulation (Swedish-German approach) and area-by-area provision of court enforceable citizen rights (the U.S. approach).

2.2. Separable Issues

There is a tendency to confuse the issues of privacy, confidentiality and security with respect to recordkeeping and computers. Dr. Ruth Davis, Director, Institute for Computer Sciences and Technology, National Bureau of Standards, outlined the essential differences between these issues and established a framework for unambiguous discussion and solution of these problems.

Privacy is a concept which applies to individuals. In essence, it defines the degree to which an individual wishes to interact with his social environment and manifests itself in the willingness with which an individual will share information about himself with others. This concept conflicts with the trend toward collecting and storing personal information in support of social programs of various importance. The government's role often makes the supplying of this information mandatory--thus, creating a direct and acute compromise of the individual's privacy. Under this circumstance, the burden of protecting personal data is all the more important.

Confidentiality is a concept that applies to data. It describes the status accorded to data and the degree of protection that must be provided for it. It is the protection of data confidentiality that is one of the objects of Security. Data confidentiality applies not only to data about individuals but to any proprietary or sensitive data that must be treated in confidence.

Security is the realization of protection for the data, the mechanisms and resources used in processing data, and the security mechanism(s) themselves. Data Security is the protection of data against accidental or unauthorized destruction, modification or disclosure using both physical security measures and controlled accessibility techniques. Physical Security is the protection of all computer facilities against all physical threats (e.g., damage or loss from accident, theft, malicious action, fire and other environmental hazards). Physical security techniques involve the use of locks, badges (for personnel identification), guards, personnel security clearances and administrative measures to control the ability and means to approach, communicate with, or otherwise make use of, any material or component of a data processing system. Controlled Accessibility is the term applied to the protection provided to data and computational resources by hardware and software mechanisms of the computer itself.

From these definitions, it is possible to see that there is no direct relationship between privacy (a desire by individuals, groups or organizations to control the collection, use or dissemination of information about them) and security (the realization of the protection of resources), although they are interrelated. Several speakers pointed out that a perfectly secure computer could be used in such a way as to violate individual privacy. However, this should not be construed as an excuse for not creating secure computer systems since the thrust of earlier remarks was to the effect that legislatively defined rules for

assuring privacy are now levying a security-oriented environment on government (and possibly private) data systems.

2.3. Social Implications

Dr. James Rule, Professor of Sociology, State University of New York at Stony Brook, presented a sociologist's view of the privacy question. He observed that the issues of privacy are social-political-human rather than technological and that the question of how far to go in computer-based recordkeeping on people is a political/social question in which the rights/needs/interests of the individual must be weighted against the rights/needs/interests of "institutions" (social, political, commercial, etc.). In his view, determining the proper balance between individual privacy and institutional needs and interests will involve even more agonizing choices in the future than it does now. To illustrate his point, he described a hypothetical situation revolving around the use of computerized recordkeeping control of crime. In the hypothetical (but potentially feasible) situation, statistical methods of behavior analysis are used to predict individual criminality before it occurs. Assuming that such a system could be assured of evenhanded administration, would such a system be desirable and would it justify the extensive recordkeeping on all individuals necessary to make it work?

2.4. Legislative Actions

As a result of the early warnings and studies of the privacy issue that have taken place in this country over the past 7 - 8 years, a number of legislative actions have taken place or are contemplated. For example, three Federal Acts have been passed in recent years relating to the issue of privacy. These are the Freedom of Information Act, which provides for making information held by Federal agencies available to the public unless it comes within a category exempted by the Act; the Federal Reports Act, which establishes procedures for the collection of information by Federal agencies and the transfer of confidential information from one agency to another; and the Fair Credit Reporting Act, which requires consumer credit reporting agencies to adopt procedures which are fair and equitable to the consumer with regard to confidentiality, accuracy, relevancy and proper use of such information. The Fair Credit Reporting Act also established the right of the individual to be informed of what information is maintained about him by a credit bureau or investigatory reporting agency.

In addition to these pieces of legislation, numerous bills have been introduced in Congress which propose to strengthen the rights of individuals with respect to confidentiality of data, prevent invasion of privacy, establish standards for the collection, maintenance and use of personal data, or limit the uses to which personal data can be put without written consent of the affected individual. It was also reported at the Conference that the Department of Health, Education and Welfare (DHEW) is implementing (internally) the

recommendations contained in the Report of the Secretary's Advisory Committee on Automated Personal Data Systems. (See Appendix B, Ref. 1)

The 50 State governments have pending numerous bills concerned with protection of individual privacy and data confidentiality. Massachusetts and Iowa have already passed significant legislation in these areas, providing higher standards of personal privacy protection than the Federal Government. Still other States have extensive legislative proposals that would impose extensive regulatory and technological constraints on the operation of personal data systems.

At the local level, a number of municipalities have passed ordinances to provide protection of computerized personal data.

While all of this legislative activity is not completed, it is indicative of the political response to the aforementioned public awareness and concern over individual rights and privacy.

2.5. Threats

Threats to individual privacy and technological threats to computer-based information systems were the two themes repeatedly stressed by the various speakers. While the threat to individual privacy and liberty was predominant and seen to be mostly associated with the unregulated collection and use of personal data, a number of the speakers cited the technological threats as being those most bothersome to the operators of information systems.

Most of the speakers agreed that the threat to privacy was one that required legal and regulatory remedies and was not basically a technological problem. All speakers agreed, however, that technology was required to help enforce the legal and regulatory steps. Furthermore, a number of speakers noted that unless there were sound technological foundations for controlled access to computer systems, the legal and regulatory actions would be largely wasted.

In addition to the basic and somewhat diffused threat to individual privacy posed by the collection and use of personal data, several speakers cited an additional problem of misappropriation and misuse of data by people who are authorized access in connection with their jobs. While the problem of misuse of data would appear to be one solved by legal measures providing stiff penalties for violators, several speakers indicated that it was in part technological since the contemporary systems have so little in the way of controlled access mechanisms that it is difficult to restrict access within a data base and to account for its access and usage.

The degree of difficulty and the costs associated with providing security and controlled access to computer-based recordkeeping systems is a function of the type of access being

permitted, the capabilities of those performing the access, and the type of computer system (whether dedicated, shared, local or remote access, etc.) on which the recordkeeping system is based. In order to put some of the later discussions of approaches to solving the problem into perspective, the classes of individuals who may access a computer system and/or its information products could be categorized as follows:

> Consumers - a term applied to the authorized recipients of information (products) of a computer-based recordkeeping system. In many applications of computers, this group is the supplier of the raw data as well. In organizational terms, consumers would comprise an operating agency or department.
>
> Producers - a term applied to the analysts and applications programmers who design and implement specific recordkeeping systems which produce information products for consumers. Producers may or may not be a part of the consumer's organization. Producers require access to the computer system to develop products; their programs require access to data in the system.
>
> Servicers - a term applied to the computer operations staff; includes operators, systems programmers, data entry services, etc., responsible for availability and maintenance of the computer system resources. The servicers may or may not be a part of the consumer's organization. Servicers require access to the computer system to operate and maintain the resource. Because they have physical access, they have the capability to access any information in or on a system.
>
> Intruders - a term applied to individuals or organizations who have no authorized access to a computer system or its products and have a possible malicious interest in obtaining unauthorized access to data or a system. Intruders are generally thought of as not belonging to any of the categories above. The primary characteristic of an intruder is his lack of authorized access to any part of a computer system or its products. He is an outsider.

The threat to data confidentiality or system security is related to the capabilities of each class of individuals in dealing with a system and the existence of an asset (data or system) that is supposed to be protected from some or all members of one or more classes. As an example, any system and its data should be protected from intruders. Some (shared) systems may contain data that is meant to be protected from different (organizational) groups of consumers, etc. A simplified view of the degree of threat and the problems faced in protecting data confidentiality and information processing resources is shown in the table and the comments following. The sixteen possible entries in the table have been grouped into ten threat classes.

Access Capability As: \ Type of System	Local (off-line) Batch		Remote (on-line)	
	Dedicated	Shared	Dedicated	Shared
Intruder	T_1	T_1	T_2	T_2
Consumer	T_3	T_4	T_5	T_6
Producer	T_7	T_8	T_7	T_9
Servicer	T_{10}	T_{10}	T_{10}	T_{10}

T_1	Intruder versus Batch	Threat is a function of physical security measures and their enforcement. High degree of risk of exposure to intruders.
T_2	Intruder versus Remote	Greatly expanded threat of unauthorized access due to potential vulnerability of communications. Low risk of exposure. Potential for masquerading as any of the authorized users quite high.
T_3	Consumer versus Dedicated Batch	Threat to data confidentiality primarily that of misusing data otherwise authorized for access. Access control based on personal identification.
T_4	Consumer versus Shared Batch	Same as T_3 plus risk of misdirecting data; control of access to data (products) generally based on personal identification by operations staff. Procedures to assure proper data handling must be available and strictly enforced.
T_5	Consumer versus Dedicated Remote	Somewhat expanded threat because of substitution of automated methods for personal identification. Also must validate identity of terminals. Requires either physical access controls for terminal area or authenticated identification of user. Increased costs of administration to control physical access to terminals and/or authenticated identification method.
T_6	Consumer versus Shared Remote	Same as T_5 with increased opportunity to masquerade if identifier/authenticator is compromised. Risk of data misroute present.
T_7	Producers versus Dedicated Systems	Producers constitute roughly the same threat as consumers except that they have the technical capability to siphon off data through corrupted programs. Degree of threat is a function of where they reside organizationally. If under same management control as consumers, threat is about the same as the consumer threat.
T_8	Producers versus Shared Batch	An increased threat to data over T_7 but generally dependent on the operating system design. Can frequently spoof the operating system to gain unauthorized access to data.
T_9	Producer versus Shared Remote	Same as T_8 (and T_7) except greatly reduced risk of exposure plus increased opportunity for anonymous bypass of access controls. Some increased risk of masquerading depending on organization and physical set-up of remote sites.

T_{10}	Servicer versus All Systems	Maximum threat. Generally unrestricted access to any program or data on the system. Greater opportunity and technical capability to access data due to direct physical access to the computer system.

III. The Operating Environment

3.1. Introduction

It would be impossible to enumerate all of the data systems involving personal or otherwise valuable data or resources. However, in order to provide an operational framework for discussion of the privacy and security issues, the Conference did provide illustrations of such personal recordkeeping functions in governmental units and the kinds of data confidentiality and computer resource security problems that are faced by Federal, State and local governments. No significance should be attached to the order in which these illustrations appear.

3.2. State of California

Mr. Kent Gould, Chief, EDP Development, Department of Finance, State of California, described the organization of data processing in California. California expects to spend approximately $100 million for data processing activities in 1973, a figure that is growing at the rate of 20% per year. Eighty (80) state departments and agencies use data processing equipment for just about every application conceivable except command and control. The Department of Finance has absolute EDP authority in California, approving individual DP budget requests for equipment and personnel. In this role, the Finance department has the responsibility for enforcing compliance with security and privacy requirements.

California is presently attempting to consolidate data processing activities into five (5) major centers. Gould estimated that between 8000 and 10,000 data bases are processed by the State of California, of which approximately 45% contain personal data. He estimated that it costs between $200,000 and $400,000 per center to provide for security and privacy requirements.

In reviewing the privacy issue as seen in California, Gould indicated that it is the responsibility of the legislature to provide policy direction in this matter and to identify the confidentiality requirements of various data. Where there is no legislative mandate, the Executive branch will take action in its best view of the problem to protect data from unauthorized dissemination and use. It will monitor the data processing practices to insure that confidentiality requirements are met. In connection with the last point, he mentioned that California was developing a master audit package that "correlates to security/privacy requirements" and will be used to measure security/privacy compliance by the operating departments and agencies.

Finally, he noted that the primary security/confidentiality problem in California is how to prevent unauthorized use of data by people having authorized access to it. The essential question is the balance between management responsibility and public responsibility.

3.3. Law Enforcement Assistance Administration

Mr. George Hall, Acting Assistant Administrator, Law Enforcement Assistance Administration, Department of Justice, reviewed the development of LEAA's activities in the development of computerized criminal information files. This activity was conceived as a network of State defined and operated systems dedicated to maintaining criminal activity information. The project grew from a feasibility demonstration project, SEARCH, that had 20 States participating by sharing criminal histories through a central data index. Hall noted that the development posed a number of design and policy questions of serious import to the question of privacy and constitutional rights of individuals. As a result of serious consideration of the problem, it was decided that: (a) the system(s) should be decentralized to eliminate the appearance (and reality) of Big Brother data banks; (b) only "serious" offenders should be included in the files; (c) only criminal and public record information should be kept. He noted that the policy decision to decentralize the system(s) has added to the costs of privacy.

In discussing the problems currently perceived with the system, a number of important problems/questions impinging on the issues of privacy/confidentiality/security were noted. Specifically, he cited the problem of who should be able to access criminal history data as one that needs joint Federal/State legislative action. Currently, most State statutes permit virtually anyone to access the records. Another problem is the integrity and validity of the data itself. Arrest records are maintained, but the disposition of the arrest is often not entered. In order to maintain properly valid and accurate data in such systems, it may be necessary to create <u>new</u> information collection systems (a move that appears to complicate the problem). Still another problem is the right of the individual to access and/or validate his records, along with questions of how long such records should be maintained. Finally, the question of file separation or merging for efficiency reasons looms large as a potential <u>future</u> danger to civil liberties.

(NOTE: The comments and problems noted above are better understood in the perspective of LEAA activity in this area. A review of LEAA's activity and other government activity in developing and maintaining criminal information files can be found in Appendix E of the HEW report.)

Finally, Hall noted a severe need for rational <u>uniform</u> standards regulating the collection and use of information.

3.4. State of Ohio

Mr. Jerry Hammett, Deputy Director, Department of Finance, State of Ohio, gave a brief review of automated recordkeeping activities in Ohio. The Ohio Department of Administrative Services either provides ADP services or authorizes the use of outside suppliers.

In describing data of security concern to Ohio State Government, he cited the following files as typical:

> Personal Income Tax Records; Driver's License Records; Arrest and Conviction Reports; VD Records (Department of Health); Patient Records (Mental Health); Government Planning Records for Highways, Buildings, and Recreation.

Indicating that the concern over the security and confidentiality of data is not exaggerated, he cited the case where a Deputy Sheriff in an Ohio county was conducting an investigation business on the side and used his access to State criminal history records to supply data to his clients. In another case, personnel in the Motor Vehicles Department were found to be expunging data of serious traffic violations from offenders' records. He also posed the hypothetical threat of having individual (and corporate) tax liability modified in an unauthorized way.

Hammett stressed his view that interactive processing threatens system security. In discussing directions for possible solutions, he indicated the need for model (and eventually real) legislation concerning privacy and confidentiality and security standards and for the vendors to provide hardware and software security in their products.

3.5. State of Illinois

In a talk on managing computer operations, Mr. Robert Caravella, Management Information Division, Department of Finance, State of Illinois, presented highlights of some of the results of the joint State of Illinois - IBM study of the applicability of IBM's Resource Security System (RSS). He began by noting (as did other speakers) that the HEW study and Canadian Task Force on Computer Security and Systems marked the beginning of a "new era" in providing safeguards for privacy and data confidentiality.

In discussing the need for confidentiality/security provisions, he cited a number of potential (and real) exposures found in contemporary systems. These include:

1. Erroneous or Misleading Data
2. Accidental Disclosure
3. Intentional Infiltration
4. Loss of Data
5. Absence of Established Standards

He then went on to outline an Information "Privacy" Action Plan. The plan outline consisted of the following steps:

1. Review Information System Requirements to Determine:

   what is collected
   why it is collected
   who needs it
   when it is needed

2. Analyze the Confidentiality and Criticality of Information:

   to operations
   for proprietary or other reasons

3. Assess Vulnerabilities and Risks - Establish Tradeoffs between:

   exposures
   value of information
   cost of safeguards
   effectiveness of safeguards

4. Make Security Decisions

5. Investigate Technical Safeguards including:

   software requirements
   hardware requirements
   physical access control(s)

6. Budget for Information Security

7. Organize for Security

8. Establish Individual Accountability

9. Implement Technological Safeguards

10. Create a Security Conscious Environment

11. Issue Policy Statements

12. Audit

Finally, in discussing the benefits to be expected from the joint Illinois - IBM security study, he noted that the project was "well-balanced" in its approach--that the vital areas of legislation, technology, administration and education were all covered in the study. In the legislative area, model legislation has been produced covering individuals' rights to privacy and regulating the collection and use of information in the State. The technology activity was focusing on the areas of performance measurement and cost analysis of using RSS. In the administrative area, the work is concentrated on monitoring the application of RSS to determine how well it meets the needs of State governments and what additional safeguards may be needed. The educational aspect is being served by the development of 10 video tape training programs aimed at diverse audiences from management to the technical support staff of ADP operations.

3.6. Department of Health, Education and Welfare

Dr. Robert Laur, Acting Director, Office of Policy Development and Planning, HEW, outlined some of the unique privacy/confidentiality problems that arise in connection with the operation of the National Center for Health Statistics (NCHS). As one of the major statistical data banks of the Federal government, the NCHS provides statistical services for HEW.

Because of the sensitivity of medical information, NCHS has adopted the isolation of a dedicated system as their approach to the confidentiality problem. The primary problem is that of data confidentiality and the protection of proprietary interests of the contributors of the data. Since the medical data is identified with a Social Security or other identification number, this number is (cryptographically) transformed to protect the identity of the individual, and the transformation key is "carefully controlled."

In support of research, NCHS provides other workers with standardized data tapes obtained from its data bases. The standardized tapes are constructed to remove personal identification and to suppress statistical entries with a small number of samples (in order to eliminate potential identification through advanced correlation techniques). In the end, Dr. Laur noted, they rely on professional ethics for the major control over how sensitive medical data is used.

He also observed that the present NCHS system security/confidentiality controls work well enough for the kind of (dedicated) systems they are now using but that they will not suffice for time-sharing systems and network connections of the future.

Presently, HEW is proposing legislation to establish a common shared information base that would let NCHS use data located at other (medical) centers (or possibly systems supporting health care delivery). This would avoid redundant collection. As an example, he cited the HEW's Professional Service Review Organization that requires correlating diverse medical, hospital and physicians' records to obtain a review. He noted that a single Federal system design for maintenance of health records raises more control problems than it solves.

3.7. Congressional Research Services

In a paper that demonstrated that requirements for data confidentiality are not unique to the Executive Branch, Mr. Robert Chartrand, Specialist in Information Sciences, Congressional Research Services, Library of Congress, provided a review of Congressional Information Protection needs. These needs are determined by the multiple roles played by a member of Congress, and the historical development of how Congress operates. Among the kinds of information cited as requiring protection were:

a) Casework data relating to individual constituents.

b) Political data--contributors lists, key civic groups, mailing lists, etc.

c) Committee/Subcommittee data--legislative planning data, privileged hearings data, etc.

d) Debate Supporting data--privileged information supporting public debate.

Supporting Congress are three computer facilities, one each for the Senate and House and the Congressional Research Service (CRS) of the Library of Congress. The Senate and House systems perform diverse administrative functions and services for the members, while the CRS system supports a variety of information systems on pending legislation, bibliographic information and an issue briefing system.

Typical of the Congressional security controls are those taken by the Library of Congress. The bulk of these are physical security measures including a visual control on computer room access, use of key-cards for after-hours work, tape vaults, burn-bags and the like. Procedural controls cited included separate handling and decentralized control of committee information, use of passwords to protect access to Congressional files, and low information content (generalized) software descriptions.

The future needs of Congress, seen by Mr. Chartrand, include:

- strengthening security provisions of legislative branch regulations
- establishing standards for need-to-know controls for all Congressional users
- description of available data and restrictions on its use
- creation of a Congressional classification system
- creation of an information service group to mediate users' information requests and enforce need-to-know and security regulations
- prepare the most applicable service and control functions which combine protection with inquiry fulfillment.

IV. What's Needed

4.1. Legislative Policies and Regulations

Legislative activity aimed at protecting individual privacy is increasing rapidly at all levels of government. As noted by Dr. Davis, passage of any significant number of these legislative proposals could easily result in an unacceptable morass of conflicting requirements being imposed on regulatory organizations, service industries and automation technology. Some national coherence in these proposals is clearly required if there is to be any realistic or

practical application of the mechanisms needed to protect against intrusions on individual privacy.

Better communication among lawmakers, government administrators, and technologists is also essential because the effective implementation of privacy legislation depends heavily upon the availability of technological safeguards that can assure compliance with a reasonable degree of certainty and uniformity. As several speakers pointed out, it may not always be possible within the current state-of-the-art to respond to legislative requirements of the type being proposed at an acceptable cost. As Mr. Gould stated, a requirement, for example, to record every access to a file involving personal data, if strictly enforced, could cause the file to double in size rapidly. Such growth clearly affects the operations of the system and inevitably leads to additional hardware and more complex software. Early coordination among lawmakers, administrators and technologists should enable impacts of this type to be taken into account in arriving at effective and reasonable legislative policies and the standards and guidelines required for implementation.

This general theme was supported by spokesmen at State and local levels of government. Mr. Andrews Atkinson, Superintendent, Cincinnati/Hamilton County Regional Computer Center, cited the need for regulations governing information management practices as they apply to data collection, storage, application, accessibility, integrity and accuracy. Mr. Carl Vorlander, Executive Director, National Association for State Information Systems spoke to the need for standards for defining categories of data requiring protection and the degree of protection required by each category.

4.2. Management and Operating Guidelines

4.2.1. Determining Information Content

Underlying the process of information management is the need to determine what information is required to carry out the function being performed and to assure that only information which is relevant and essential to that function is collected and processed. The weeding out of nonessential confidential information through this process obviously contributes directly to easing the problems of privacy and data security and thus represents a management activity that should be pursued vigorously and continuously. The processes of security management, as discussed in the Conference, exclude questions of information content but recognize them as important and interrelated considerations which must be addressed.

4.2.2. Evaluating Risks, Threats and Security Techniques

Assuming that the essentiality of the data to be protected has been determined, management guidelines or operating procedures are needed for the effective employment of proper security measures. Particularly needed at this time are guidelines for determining the level

of confidentiality or criticality of information (i.e., what degree of protection is required for proprietary, personal, high value or sensitivity reasons). Of equal importance, as noted by Dr. Walter E. Simonson, Associate Director of Electronic Data Processing, Bureau of the Census, are guidelines for assessing the risks and threats to security, identifying the assets to be protected and evaluating the relative effectiveness of alternative safeguard measures in providing that protection. Dr. Simonson emphasized that employees constitute a major potential threat and suggested the use of pre-employment screening to minimize this risk.

A variety of management techniques exist for valuing assets; and if that were all of the problem, it would be a straightforward actuarial problem to design the required level of security. However, when data confidentiality is part of the security problem, factors other than simple asset replacement costs have to be considered. Some of the factors involved include the degree of threat posed by different potential accessors of a system, as was discussed in Section 2.5.

The specific techniques to be used obviously depend on the degree of threat (or on the degree of confidentiality or importance of the data being protected). Most systems have only the most rudimentary controlled accessibility features. While it can be argued that the cost of providing protection techniques to a data base should be borne by the application(s) requiring them, the design of contemporary systems too often permits such controls to be bypassed completely by anyone with a programming capability. Where the systems are used with a clear and strict distinction between consumers of information and producers of the applications, various data base protection techniques can protect data from unauthorized access by consumers. In many systems, consumers are often producers as well.

However, there are many questions that must be resolved even where the consumers are distinct from the producers. Whether the computer-based protection techniques should be applied on a per-application basis or whether these techniques should be an integral part of the operating system are questions that management of data centers need trade-off evaluations to answer.

The relatively simple question of how to represent authorization to use a data base becomes quite complex depending on the level of detail to which the authorization must apply--file, record, or field within a record. Methods for representing such authorization must be designed and evaluated in the context of the organization and intended use of data bases. Equally important, the management and administrative procedures to update, review and otherwise control the authorizations need to be developed for the technique(s) chosen.

Currently, most of the effort to provide such controls is carried out by the users of data processing systems. Whether they or the suppliers of data systems should develop such protection mechanisms, the fact remains that data center managers have no guidelines as to which kind of controlled accessibility techniques to use under different circumstances and no

statements of the assumptions underlying assertions of protection provided by any particular technique.

4.2.3. Physical Security

The objective of physical security is to keep intruders away from data processing and information resources, as well as to protect the resources from natural hazards. Mr. Ike Friedlander, Executive Director, Public Building Services, GSA, noted that physical security is the foundation of nearly all other security solutions. If physical security measures are not taken, then external penetration of systems can easily occur, making most other measures of doubtful value. He stated that technological detection systems are being used more frequently because of the increasing costs of using human guards. In new construction, physical security is an important design criterion. In some cases, such as a new government building in Seattle, the security system is controlled by a dedicated computer.

The major emphasis in physical security technology is the development of products designed to reduce the cost of a human guard force by providing means to supplement or extend their capabilities. Thus one finds the increased use of closed circuit TV, ultrasonic and other alarm systems, walkie-talkies, smoke and heat detectors of various kinds and the like.

Interestingly enough, there is little in the way of new technology needed for physical security. Mr. Nicholas A. Chronis, Chief, Data Processing Computer Center, Civil Service Commission, pointed out that "the technology exists if the money is available." The major need he see is for Federal guidance on how to provide day-to-day physical computer security. The National Bureau of Standards is planning to publish such guidance early in 1974.

4.3. Controlled Accessibility

Mr. Walter W. Haase, Deputy Assistant Director, Information Systems, Office of Management and Budget, summed up the focus of controlled accessibility in his introductory remarks at the Panel on Controlling Access to Systems and Data when he said:

> "I believe that proper application of existing computer, communication and information processing technology can reduce the threat of improper disclosure of private and confidential data. I also believe that further development effort is required to close the gap between access control needs and available technological solutions. I am not suggesting that technology can provide a solution to the basic privacy issue but that it could reduce the intensity of the conflict."

As described by Dr. Dennis Branstad, Computer Security Project, National Bureau of Standards, the term "controlled accessibility" embraces the technological measures available to control the access of people to a computer system's data and computational resources. These measures include specialized hardware and software, access procedures, authorization

mechanisms, identification methods, and encryption algorithms. Only computer-based mechanisms can provide the rapid response decisions needed for effective access control.

In discussing what is needed to protect data confidentiality in computer-based record-keeping systems, Mr. Daniel Edwards, Research Engineer, NSA, and Mr. Howard Lewis, Manager, Data Management Programs, AEC, both noted that access to the following must be controlled:

a) Computer sites and mainframes.

b) Terminal sites and terminals.

c) Storage facilities

d) Files and records.

e) System and application programs.

f) Computer output.

g) Telecommunications.

Further, the controls must be applied to people, terminals and programs.

4.3.1. Identification of Individuals

The underlying basis of information processing resources protection is unique identification of an individual. Authorization to access data, obtain information products or use information processing resources is ultimately based on such identification. The techniques available or being actively pursued are quite extensive. They include use of picture badges, magnetic striped credit cards, passwords, fingerprint readers, hand geometry readers, lip print readers, voiceprint recognition equipment, dynamic signature analysis and the like. The identification techniques are applied to supplement or replace human recognition of an individual attempting to gain access to a building, computer room, terminal area, terminal, computer (from a remote site), etc.

Clearly some identification techniques can serve multiple purposes (e.g., magnetic striped cards can be used to control door locks (and as an identification to a computer), while others are limited to a single function (e.g., passwords as a means of identifying an individual to a remote computer or as a method of authenticating access authorization to files).

It is generally true that identification techniques based on something tangible (e.g., a badge or a fingerprint) can be defeated by duplicating the identification. Thus the problem of "breaking security" is transformed into the often simpler task of duplicating or simulating a physical entity.

In general, the methods of automated identification that do not require human perception (magnetic card readers, fingerprint readers, etc.) often involve high implementation costs, so it is often economically feasible to apply them only where there are relatively few points (rooms, terminals, etc.) where such identifications must be made.

The intangible methods of unique identification (passwords and catechetical sequences) have the advantage of not requiring input apparatus but are not as broadly applicable as some of the tangible methods. Primarily because of their low implementation cost and simplicity, intangible identification methods are frequently used in time-shared systems serving a large, frequently changing, geographically dispersed population.

The choice of which methods to use for unique personal identification involves criteria such as user convenience, cost, precision of identification, the number of points where identification must be made, etc. Criteria for evaluating and using such schemes are needed because of the critical role unique identification plays in all aspects of security.

4.3.2. Authorization Mechanisms

Both Mr. Lewis and Mr. Edwards emphasized the need for authorization mechanisms to control access to systems. These mechanisms are often programs that validate a user's (and/or program's or terminal's) right to use a given element being protected (e.g., data, program, terminal, etc.). Mr. Lewis noted that "in practically all cases, the off-the-shelf computers and control programs supplied by the manufacturers have inadequate protection mechanisms for providing controlled access to a computer's assets." Mr. Edwards supported this view and added that most computer systems are sold as complex and expensive do-it-yourself kits.

Examples given of authorization mechanisms included those to validate initial access to a system (e.g., from a terminal), validation of data transmission to a terminal or user (i.e., assuring that both the user and the terminal are "cleared" to receive the data accessed), and validation of access to files (including program files), records and fields.

While many contemporary systems have one or more specific authorization mechanisms (e.g., password validation of terminal users), the mechanisms are not applied uniformly in response to a general security principle. This results in the users having the choice of building their own control programs or modifying that supplied by the vendor in order to obtain the level of controlled access they need. Neither of these alternatives is especially attractive.

Another consequence of the piecemeal "Band-Aid" approach to providing security "features" on contemporary systems is the dispersal of the authorization mechanisms into a variety of control and applications programs. Because controlled access is not a design requirement for the operating system, it is not surprising that current systems have many "holes" caused by incomplete application of the controlled access principle. These "holes" can be exploited by

virtually any programmer to circumvent the security "features" and existing authorization mechanisms to gain unauthorized access to data, programs, or the operating system itself. Of some six (6) to eight (8) penetration exercises run against a variety of machines, all of them achieved undetected unauthorized access to files and programs or supervisory control of the target system.

4.3.3. Technological Needs

Mr. Lewis and Mr. Edwards indicated that in order to meet the stringent requirements of providing data confidentiality (especially in universal access utility systems), it is necessary to have computer systems and control programs (operating systems) built with controlled access or security as a major design goal. In order for users to be able to evaluate the products being offered, it would be necessary for the vendors to supply detailed security specifications that include the (assumed) security perimeter, the external and internal protection mechanisms provided, what they protect from whom, and how the protection is achieved. The goal is to achieve a penetration-proof system with protected authorization mechanisms that permit precise and continuous validation of all access in the system.

It is also necessary to provide systems that can be "certified" to be secure by some independent authority. Drawing on the analogy of the rating of safes and storage containers as being able to resist various attacks (e.g., dial manipulation--20 man-minutes, forced entry--0 man-minutes), Mr. Edwards pointed out that proof (of security) by emphatic assertion will not suffice. It must be possible to convincingly demonstrate that a system is secure under various kinds of attacks. There is also the need to be able to recertify a system in use because of the almost continuous stream of changes that take place in the hardware and software of an operational system.

The primary thrust of the remarks was directed at the requirement to obtain systems that provide protection even against the threats posed by persons with the authorization and capability to produce their own programs (producers). However, even for less demanding environments where protection is required for intruder and consumer threats, much more needs to be done. In particular, the evaluation of already existing technological alternatives for retrofitting existing systems with controlled accessibility mechanisms that are appropriate for the degree of protection required and the potential threat source (intruders, consumers, producers, etc.) is needed now.

4.3.4. Network Security and Cryptography

The controlled access problem is not confined to computer systems alone, as the discussion regarding controlled access and security of the telecommunications networks linking computers and users brought out.

Mr. Charles Joyce, Assistant Director, Office of Telecommunications Policy, in outlining the problem, indicated that the basic network security question to be resolved is what proportion of protection responsibility should the communications subsystem bear.

Dr. Michael Muntner, Director, Advanced Planning and Research Division, Automated Data Management & Telecommunications Service, GSA, noted that virtually all current effort is focused on the terminal end of networks since that is where the bulk of the experience has been. It was his contention that access control requirements are best handled as part of an initial systems design rather than by patches and repairs to systems and networks after the fact. He presented three types of network situations that reflect three different kinds of management control of the resources involved. These were:

a) An integrated system--a single management responsible for both computer systems and telecommunications control.

b) Segregated systems--one management is responsible for only the network and a different management is responsible for the computer (based) resources.

c) Hybrid systems--where one management is responsible for some of the computer (based) resources and the network, while other managements are responsible for the remaining computer (based) resources.

These divided management responsibilities underscore the difficulty of assuring that the security and controlled accessibility of a network of computer (based) resources is properly achieved. It also underscores how the allocation of responsibility for security between the systems and the network can result in each believing the other is (responsible for) taking care of the problem. The basic issues involved in a particular network are:

1. How well the computer systems protect themselves.
2. How deeply can encryption be incorporated into the network.
3. Whether security-related functions can be standardized across all system elements.
4. What records should be kept.

Of these points, 2 and 3 are the most important to networks in general, particularly where the composition of the network is not homogenous in equipment.

Dr. Davis pointed out that cryptographic techniques can be used to protect data during transmission among systems. Cryptographic transformations can be applied to protect data transmitted between a computer and its terminals or other computers. The transformation can be applied to passwords or even data in storage.

Details of cryptographic transformations and their applications have not received wide circulation among civilian (nor most government) information systems developers. As a consequence, users have no basis for evaluating the efficacy of one proposed technique over another. As an example, one manufacturer of commercial scramblers (cryptographic machines) used a simple linear shift register as the generator of the cipher key. Current papers have appeared recently showing how simple it is to "break" such a system with as few as 2N bits of key (where N is the length of the shift register).

In addition to needing an evaluation of the strengths of specific cryptographic techniques, it is also necessary to evaluate whether or not they can meet other protection objectives such as preventing effective alteration or replacement of all or part of the message, or detecting attempts to retransmit previously sent legitimate messages, or denying intrusion on common carrier networks.

The controlled access problems that exist in stand-alone computer systems are quite formidable in their own right. When computers are linked to terminals and each other, there are the considerable additional problems of determining whether attempted user accesses are legitimate and even who is attempting access. Where the interlinking communications system is a switched common carrier (e.g., the telephone network), the opportunities for remote penetration for intercepting data is increased significantly.

The primary needs for network security are criteria that relate costs of data confidentiality to the type of network, inexpensive security techniques (e.g., cryptography) that can be applied to networks of heterogenous equipment, methods of authenticating users and computers which are not susceptible to masquerade, and model secure network designs that clearly identify what protection is provided by the network against specific kinds of threats.

4.4. Computer Security Auditing and Surveillance

A number of speakers mentioned the need for security auditing of information processing systems as a management tool for enforcing data protection policies.

In a discussion of evaluating existing systems, Mr. Robert Abbott, Manager, RISOS Project, Lawrence Livermore Laboratories, focused on the need to audit existing protection mechanisms. In discussing the problems this poses, he cited the lack of data on the experiences of others using contemporary systems and the vast size of current operating systems as discouraging for such analysis.

It was pointed out by Mr. Abbott that pre-use auditing of existing protection mechanisms requires collaborative arrangements with manufacturers that enable the auditors to obtain accurate information about the system under study. The main barrier to such cooperation currently would appear to be the lack of suitable arrangements that protect the proprietary

and marketing interests of the manufacturers while providing system auditors with the information needed to evaluate a system in a way that protects its integrity.

In other discussion of auditing the use of systems, several speakers noted the importance of such audits in determining proper use of an information processing resource. Mr. Gould stated that California was developing a master audit package that would measure users' compliance with the security/privacy requirements established for their data. Dr. Branstad also spoke of the use of surveillance and audits to maintain accountability for resource usage and data access.

In the areas of monitoring usage and data access accountability and compliance with protection standards, a major problem is that security auditing is attempted from the operating systems instrumentation for accounting. While much of the same information is needed (e.g., identification of who is using the system) for both purposes, security auditing techniques may require more detailed information on just how a system is being used (e.g., what language processors are used, what physical devices are used, etc.) than that required for accounting purposes alone. An existing technological problem is how to instrument both the hardware and software of a system in such a way that very specific and detailed information on what a user is doing can be selectively recorded without disturbing the operating environment for all others. If this becomes feasible, an effective interface to the systems' management must still be provided which permits specification of the activity to be monitored for a user, device, terminal, line, etc.

V. Costs

5.1. Introduction

The importance of information in our service-oriented society leads to a consideration of the social costs of limiting access to data in the interest of protecting individual privacy and data confidentiality. Since data collection is often required to plan and operate needed service programs, lack of accurate data will either inhibit the development of these programs or raise the costs of implementing and operating them. Either way, there is a cost associated with any "solution" that involves indiscriminate suppression of recordkeeping or makes the operating costs too high by imposing unrealistic standards of data confidentiality and control. These factors are beyond the scope of this summary.

There is a strong indication that the public is willing to pay in some way for privacy and security. Dr. Davis noted that approximately 15% of the telephones in the U.S. have unlisted numbers for which the subscribers pay various rates varying from a $9.00 fixed charge to 50¢ /month. On a less discretionary basis, passengers on national airlines have been paying a surcharge on fares for airport security and anti-hijacking measures. Other widely used services which have a cost component for privacy or security include: recreation, housing, health, education and local (commuting) travel. From these broad-based examples, it is

possible to conclude that the costs for maintaining personal data confidentiality and security in government-operated information systems will be readily borne by the public. As Dr. Davis pointed out, however, the question of cost allocations among the public, industry and government has rarely been addressed. Such studies are needed to form the basis for privacy decisions and the development of appropriate cost allocation schemes.

5.2. Costs of Security

5.2.1. Physical Security

The costs of physical security are more easily identified than the costs for other areas of computer security. Physical security costs include constructing limited access sites for computers and terminals, vaults for tape and disc storage, additional costs for fire detection and suppression and the like. Most of these costs should be allocated to the protection of data processing resources rather than to the protection of data confidentiality. One would expect these measures to be in force independent of the additional need for data confidentiality. Because computers represent an important asset of an organization, they require protection at a level which is at least equivalent to the value of the equipment.

Carefully designed and implemented physical security will provide adequate protection of information processing resources and data bases from intruders. The costs of physical security are a relatively small part of preparing a site for a computer system.

As noted previously, an objective of physical security is to prevent unauthorized individuals from physically accessing a computer system or any of the file media, terminals, etc. As a result, the major additional costs beyond those associated with protection of assets from natural disaster are associated with personnel identification and physical access control. For many systems, a policy of locking the computer room and restricting access to just operations personnel only provides a large increment of security for the system. Mr. Chronis deplored the open showcase kind of installation that results from management being insensitive to the needs of security.

5.2.2. Controlled Accessibility

It is in this area that discussion of costs becomes more emotional than objective. It is sometimes stated that you can design for security and compromise performance or design for performance and compromise security. The problem, of course, is to design for both.

A number of people claim that serious cost penalties are associated with computer security. This was implied in the remarks by Mr. Kenneth Orr who indicated that it was necessary to determine when and how to trade off performance for security. This view comes about in part from acceptance of the fact that access control mechanisms have to be imbedded deeply in the

internal operating systems to provide the computer systems with a large measure of self-protection. The current thinking of the technical community is that the primary way this can be achieved economically is to adapt, modify or change the architecture of the computer system to provide a hardware data access (reference) validation capability in the form of segment tables, descriptors, or address mapping hardware with associated authorization controls. Any attempts to achieve complete data access validation (including that within the operating system) in software alone would indeed raise the execution overhead to an unacceptable level and would also be very costly in terms of additional programming for the reference validation(s). A software-only approach makes it imperative that the software design and implementation be done correctly.

Another aspect of the costs of security was brought out by Mr. Edwards who cited that attempts to "fix" operating systems by patching them are fruitless exercises because the patches are generally repairing a symptom rather than the underlying cause. Because most present efforts at security are patches and additions to a basically unsound foundation, they are fairly easily defeated. Based on his observations of a number of penetration exercises, he estimates the cost of "breaking" a system at roughly 1/10 the cost of creating and installing patched protection mechanisms.

Mr. Abbott indicated a cost of 18 man-months to do a "good integrity study" of a system with up to 6 months of study required to become familiar with the system under investigation. This level of effort is needed to just identify major potential problems.

Still another indication of the cost of security is found in the Air Force Security Technology Planning Study (4) which indicates that the cost of "repairing" a single contemporary system, removing all of the known security deficiencies in the system, is on the order of 2.5 million dollars. As a further indication of the magnitude of these costs, Mr. Gould indicated that the costs attributable to security in the five super centers being developed in California were from $200,000 to $400,000 per center over and above the costs attributable to physical security.

The argument that making systems secure is costly is valid if the systems' architecture does not provide any hardware assistance to enforce the access control protection of the system. In this situation, the cost in performance and other tangible factors that would have to be passed onto the customer is quite high.

There are, however, computer systems with the necessary architectural embellishments that would make it possible to achieve the level of self-protection needed to support access control and authorization mechanisms in a reliable and secure way. Even in these, because security has not been a paramount issue in the design of the operating system, the features most often are haphazardly used. In these kinds of systems, the performance degradation attributable to security is expected to be quite low because the architectural features of utility for security are included for other purposes--primarily for dynamic memory allocation.

Once one has achieved a self-protected system, it is then possible to consider a variety of added authorization mechanisms needed to control the employment of the resources of the system. A self-protected system is not of itself a secure system--rather it is a reliable foundation upon which to build a secure system for given applications.

5.2.3. Communications Safeguards

Communications can be protected either by physically protecting the transmission lines or by using cryptographic devices. Physical protection of the lines is feasible if all remote users are located in the same facility as the computer center. The incremental costs of physical protection of communications lines can be quite small if the overall physical security of a site is good.

The cost of encrypting message traffic among computers and terminals includes the costs of the cryptographic equipment itself and the increased administrative costs of protecting the keying information. It is necessary to physically protect the cryptographic device from unauthorized access or tampering as well, but this cost may be minimal if the remote site already has adequate physical protection.

Typical commercially available cryptographic devices or scramblers cost in the range of $2000 to $5000 per unit, with discounts usually available for quantity orders. Where only a few lines are protected in this way, there is no special problem encountered. However, when it is necessary to protect a large number of lines, then the costs of having a scrambler at both ends of every link become significant. None of the manufacturers of this equipment have developed multiplexed cryptographic techniques for this kind of application. Scramblers based on simple principles can sometimes be simulated in a computer, thus achieving the desired multiplexing. However, this appears to be possible only for those scramblers whose principle is also susceptible to simple analysis and exploitation.

Basically, the communications protection costs can be easily ascertained if the need is recognized.

5.2.4. Costs of Not Providing Technological Safeguards

As the need for data security is recognized and legislation is enacted to protect data confidentiality, governmental agencies will be faced with establishing stringent data-handling procedures to protect this data. Without technological safeguards which can provide this protection, other "stop-gap" measures must be used. The costs resulting from using these measures on contemporary systems are:

- inefficient utilization of existing hardware and personnel, or the acquisition of extra hardware and personnel to maintain separation of protected data

- loss of information accuracy, timeliness and completeness resulting from reduced data sharing and inadequate data correlation brought about by having to maintain separation of protected data from other data.

Specific operational procedures being used and the cost incurred for providing security and data confidentiality for highly sensitive or valuable data include:

- separate computers for separate applications to achieve isolation, when combined operation on a single machine would otherwise significantly reduce costs;
- sharing of a computer by several applications sequentially instead of concurrently, resulting in costly change-over procedures;
- scheduling applications involving protected data at times when time-sharing terminals are disconnected;
- restricting capabilities of users at remote terminals.

These practices require substantially more equipment and personnel than would be required for operation on self-protecting resource-sharing systems. Not only are the direct equipment and people costs increased, but so are the costs resulting from reduced operational effectiveness. It is estimated that the increased costs resulting from these practices range between 10% and 100% of the costs of operating an installation, with an average cost estimate of 40%.

VI. Action Plans

6.1. Introduction

Progress toward resolving the governmental needs and problems identified during this Conference requires the coordinated efforts of the nation's legislatures, government management, the service industries, and the automation industry. A realistic approach to providing solutions could consist of parallel and coordinated efforts directed toward:

- Achieving a national coherence among laws defining the privacy rights of individuals and the basic information practices to be followed in protecting these rights.
- Establishing uniform management and technical procedures and guidelines for the effective application of security measures.
- Innovative applications of existing technology to enhance security mechanisms and techniques.
- Research and development where the technology needed to eliminate serious security deficiencies does not exist.
- Studying and allocating costs of confidentiality and security in automated information systems.

6.2. Cohesive Legislation

A national legislative conference called for the purpose of considering the adoption of uniform legislative policies, definitions, requirements and penalties would represent a significant contribution to assuring the effective implementation of laws that are enacted.

Specifically needed are definitions of the rights to be accorded to individuals in the collection, use, and dissemination of personal data and the disclosure of information to the individual for purposes of verification. The recommendations of the HEW Advisory Committee could serve as a point of departure for such a conference (see Appendix A). An expected outcome of the conference would be model Federal, State, and local legislation for addressing the privacy problem. A number of such models are in existence. These could be considered and either recommended or modified as required.

In formulating model legislation or specific proposals, it is essential that the legislative branch at all levels of government have the advice of the technological community to assess the technical feasibility and impact of proposals designed to protect data confidentiality. In addition to the expertise of the appropriate government technical organizations, the computer technical societies, such as the Association for Computing Machinery and the Computer Society of IEEE, should make their resources available to interested legislative committees.

6.3. Uniform Management and Operating Procedures

Cooperative efforts among government agencies, professional societies, computer industry and private sector groups, such as the American Banking Association and the American National Standards Institute, can result in the early agreement, documentation, and widespread distribution and implementation of useful management and operating procedures.

In particular, efforts should be directed toward determining levels of data confidentiality required for the protection of privacy rights and their impact upon technological support requirements. Since these levels can be expected to vary among special user communities, such as health, law enforcement or credit services, initiatives can be exercised by these communities in cooperation with the computer and information technologies.

Of broader and more common application are techniques for such activities as assessing risks, determining threats and threat sources, evaluating alternative security measures, auditing and physical security. Some of these techniques already exist and could be readily documented for wide dissemination and use. As an example, the National Bureau of Standards is developing physical security guidelines which will be made available through public distribution channels. Other organizations with documented techniques could offer them for use elsewhere or, working jointly, could speed up development of techniques which are not now available.

Models of computer system and data protection measures that could be used against various threats would be extremely helpful in providing management with ready-made designs for the operation of secure automated data systems that could be adapted to meet local needs.

6.4. Research and Development

Interaction among government agencies, other user communities, and industry groups can lead to general agreement on significant needs and problems which cannot be satisfied by existing science and technology. Research and development efforts to fill these gaps could proceed on a coordinated but independent basis.

This Conference has initially identified several such needs. Among these is a need for self-protected computer systems. While techniques for controlled accessibility exist for systems which are not programmed by their users, little is being done to generate self-protected systems as a base for resource-shared systems which are secure against threats by producers (where programming access is provided to some or all users). The focus of ongoing efforts is to develop secure advanced time-sharing systems supporting on-line programming, extensive program-sharing facilities and the like (such as the Air Force project to develop a certifiably secure system and a multi-mini computer system, such as that being developed at the University of California, Berkeley.)

In addition to this important work, there is a need to develop self-protected systems on other suitable equipment. In order to accomplish this, it is necessary to define uniform self-protection requirements and to develop models of controlled accessibility that are based on other modes of computing, such as multiprogrammed use of systems with data file sharing in production environments.

Secure operating systems are those with access authorization mechanisms which use the system's self-protection mechanisms to enforce the access limitations of a programming user (producer). In such a system both the self-protection and access-authorization mechanisms must be self-contained and certifiable. One expression of these concepts is found in the Air Force Computer Security Technology Planning Study. It postulates systems in which all references of any program to any other program, data, or peripheral device are validated during execution against a list of authorized types of reference based on user and/or program function. This idea is called a reference monitor concept and is to be realized in a combination of hardware and software called a reference validation mechanism.

It is the efficiency consequences of the requirement for validating each reference of an executing program that leads to a search for hardware techniques to perform this function. For this reason, descriptors or address mapping tables that include reference-type checking appear attractive for developing secure systems.

The software components of a reference validation mechanism include the processing of authorized references for each user/program function to set values in the tables/descriptors used in reference checking, software that provides for the administration of the authorizations for individual users, and software that deals with attempted violations of authorized access.

Another need for further research and development relates to network security. The outstanding needs of network security are not generally understood by either users or the technical community at large. Not only is the security of information processing systems connected via a network at stake; but the network, itself, becomes an object of security interest. A coordinated research program to provide secure network models which can be used to measure and evaluate costs, protection, and service would help designers to decide where to allocate any security-related functions to the network and, if so, which ones (e.g., user identification, authorization checks).

Finally, the inability to positively and uniquely identify individuals who are authorized to gain access to computer systems and data remains a basic obstacle to computer security. Further research and development of identification techniques, together with network security and self-protected systems, represents an initial set of requirements around which, by common consensus, a coordinated program can be pursued.

6.5. Innovative Applications of Technology

Innovative applications of existing technology can produce improvements in the capability of currently available systems to protect data. Cooperative efforts among users, user communities and the computer industry to develop and stimulate new ideas and to publicize successful experiences can make a positive near-term impact upon security effectiveness.

Two such possiblities were identified at this Conference. The first relates to the retrofitting of existing systems to satisfy new security requirements.

On most systems, for example, it would be fairly easy to validate a program's authority for initial access (e.g., OPEN) to a given file or a user's authority to call for the execution of a given program. Because these validation functions would occur only once per job, they are not too costly to consider using and would provide at least a first level of controlled accessibility for a system. It would be possible but more difficult to provide validation of authority to access specific records of a file since it would require a representation of the access privileges accorded to the use of a file (e.g., records could be individually tagged for reading only) or to each record by a label which shows in some meaningful way the kinds of restrictions on its use.

Where the individual making the access is a consumer only, record access validation can be still relatively simple. However, the complexity increases if record access validation is applied to producers who can generally request any processing action on a record (e.g., read, write, delete) and whose authority to access a record has to be determined in the specific context of the request.

While centralized authorization mechanisms will not solve all possible controlled accessibility problems for any particular system, they will provide greater data security on systems than is presently available and in many cases will be adequate in the short run.

A second possibility for the innovative application of existing technology involves the use of cryptographic devices and data encryption techniques. The National Bureau of Standards is currently engaged in making available encryption algorithms to provide a way for civilian agencies of government to protect the contents of data during storage and transmission. Related to the use of these techniques is the need for low-cost effective cryptographic devices that can be used to protect data confidentiality and integrity in systems using telecommunications. With the availability of self-protected systems, programmed encryption techniques become viable as a means of protecting data on physical storage media or between devices with computational capability. However, such techniques impose additional burdens of key management that need cost-effective resolution. Therefore, development of techniques for efficient key management are also needed.

6.6. Cost Allocations

A study of the costs of data confidentiality and security in automated systems is essential in creating an understanding for making public choices about the privacy needs of individuals and for allocating the costs among the suppliers, the user communities, the public and the government. Costs must be identified and acceptable concepts developed for cost allocations schemes. Since these will undoubtedly vary among such service activities as government, banking, credit and medicine, appropriate studies might logically be organized on this basis and participated in by management, economists, and technologists.

Appendix A

CONFERENCE PROGRAM

Monday, November 19, 1973

8:15 a.m. Conference Registration

9:30 CONFERENCE INTRODUCTION

Welcome: Dr. Richard W. Roberts, Director, National Bureau of Standards

Keynote Remarks: Honorable John K. Tabor, Under Secretary of Commerce

The Congressional Interest: Honorable Jack Brooks, Chairman, Government Activities Subcommittee, Committee on Government Operations, House of Representatives

A Statement of the Problem: Dr. Ruth M. Davis, Director, Institute for Computer Sciences and Technology, National Bureau of Standards

10:30 - 10:45 Break

10:45 - 1:00 SAFEGUARDING PRIVACY
Mr. David B. H. Martin, Session Chairman
Special Assistant to the Secretary
Health, Education and Welfare

Governmental Systems with a Need for Privacy Protection

Federal: Mr. George Hall, Acting Assistant Administrator, Law Enforcement Assistant Administration, Department of Justice

Municipal: Mr. Andrews Atkinson, Superintendent, Cincinnati/Hamilton County Regional Computer Center

Issues and Requirement for Privacy Safeguards

Professor James Rule
State University of New York

A California Solution

Mr. Kent Gould, Chief, EDP Control & Development, Department of Finance, State of California

1:00 - 2:15 Lunch

2:15 - 5:15 CONTROLLING ACCESS TO SYSTEMS AND DATA
Mr. Walter W. Haase, Session Chairman
Deputy Assistant Director, Information Systems,
Office of Management and Budget

The Need and Significance of Controlled Accessibility

Dr. Dennis Branstad, Project Leader, Computer Security, National Bureau of Standards

Governmental Systems with a Need to Control Access

Federal: Dr. Robert Laur, Acting Director, Office of Policy Development and Planning, Health, Education and Welfare

State: Mr. Jerry Hammett, Deputy Director, Department of Finance, State of Ohio

Congress: Mr. Robert Chartrand, Science Policy Research Division, Congressional Research Service, Library of Congress

Providing for System, Program and Data Integrity

Mr. Howard E. Lewis, Jr., Manager, Data Management Programs, Atomic Energy Commission

Managing Computer Operations

Mr. Robert Caravella, Management Information Division, Department of Finance, State of Illinois

Tuesday, November 20, 1973

8:15 a.m. Conference Registration

9:00 - 10:30 CONTROLLING ACCESS TO SYSTEMS AND DATA (cont'd.)
Mr. Charles Joyce, Session Chairman
Assistant Director, Office of Telecommunications Policy

Controlling Access to Local Computer Systems

Mr. Daniel J. Edwards, Research Engineer, National Security Agency

Controlling Access to Computer Networks

Dr. Michael Muntner, Director, Advanced Planning and Research Division, Automated Data Management & Telecommunications Service, General Services Administration

10:30 - 10:45 Break

10:45 - 11:30	INTERNATIONAL ACTIVITIES RELATED TO PRIVACY Dr. Alan F. Westin, Professor of Public Law and Government, Columbia University
11:30 - 1:00	REQUIREMENTS FOR PHYSICAL SECURITY Mr. Ike Friedlander, Session Chairman Executive Director, Public Buildings Service General Services Administration
	Records and Personnel Management
	Dr. Walter E. Simonson, Associate Director of Electronic Data Processing, Bureau of the Census
	Protecting Against Environmental and Other Hazards
	Mr. Nicholas A. Chronis, Chief, Data Processing Computer Center, Civil Service Commission
1:00 - 2:15	Lunch
2:15 - 3:45	ASSESSING SECURITY RISKS AND COSTS OF PROTECTION Mr. Carl Vorlander, Session Chairman Executive Director, National Association for State Information Systems
	Auditing Existing Protective Measures
	Mr. Robert P. Abbott, Manager, RISOS Project, Lawrence Livermore Laboratories
	Management Evaluation of Needs, Benefits and Costs of Security Protection
	Mr. Ken T. Orr Topeka, Kansas

Appendix B

Publications/References Cited at the Conference

1. "Records, Computers and the Rights of Citizens," Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education and Welfare, July 1973, U.S. Government Printing Office (Stock No. 1700-00116), Washington, D.C. 20401, Price $2.35, postpaid.

2. Federal Fire Council Publication RP-1, "Fire Protection for Essential Electronic Equipment," available from: National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, Virginia 22151, under document number AD-692-662. Price $6.00.

3. DOD Directive 5200.28 and appendix 5200.28 M. Office of the Secretary of Defense, the Pentagon, Washington, D.C. 20301.

4. "Computer Security Technology Planning Study," October 1972, Electronic Systems Division, L.G. Hanscom Field, Bedford, Massachusetts 01730, ESD-7R-51, Vol. I and II.

5. Report of GUIDE Subcommittee on Security Requirements.

6. Project SEARCH Security and Privacy Publications available from: Project SEARCH, CCTRF, 1927 13th Street, Sacramento, California 95814.

7. GMIS Project 73 publication: An Administrative Guideline for Security and Confidentiality in State and Local Government Data Centers, GMIS, 138 East Court Street, Cincinnati, Ohio 45202, price $25.00.

Appendix C

Preview of Conference on Privacy and Computer Security
National Bureau of Standards, Gaithersburg, Maryland
March 4-5, 1974

This Conference is planned as a sequel to the November 1973 Conference to continue the dialog and interaction among government, industry and public interest groups that is needed for effective resolution of the privacy and computer security issues.

More specifically, this Conference provides an opportunity for the computer industry and other groups in the public and private sectors to present solutions, ideas, and approaches for dealing with the governmental needs and problems outlined in this Conference Report. The suggestions may include legislative, technological or managerial measures, and may focus on existing state-of-the-art techniques, advanced methodologies currently under development or promising research interests of a longer range nature.

Participants in the program will include persons from:

- The Congress
- State legislatures
- Individual computer companies and consulting organizations
- Professional organizations
- Academia

Attendance at the Conference is open to all interested persons, including management and technical personnel from Federal, State, and local governments, the computer industry, public interest groups, professional associations, academia and privacy and security experts.

Further information may be obtained from the Conference office:

NBS Privacy and Computer Security Conference
Administration Building, Room 209A
National Bureau of Standards
Washington, D.C. 20234

Phone: (301) 921-3195

U. S. GOVERNMENT PRINTING OFFICE : 1974 O - 531-849

NBS-114A (REV. 7-73)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET	1. PUBLICATION OR REPORT NO. NBS TN-809	2. Gov't Accession No.	3. Recipient's Accession No.

4. TITLE AND SUBTITLE

Government Looks at Privacy and Security in Computer Systems. Summary of a Conference held at the National Bureau of Standards, Gaithersburg, Maryland, November 19-20, 1973

5. Publication Date

February 1974

6. Performing Organization Code

7. AUTHOR(S)

Clark R. Renninger and Dennis K. Branstad, Editors

8. Performing Organ. Report No.

9. PERFORMING ORGANIZATION NAME AND ADDRESS

NATIONAL BUREAU OF STANDARDS
DEPARTMENT OF COMMERCE
WASHINGTON, D.C. 20234

10. Project/Task/Work Unit No.

640.1110

11. Contract/Grant No.

--

12. Sponsoring Organization Name and Complete Address *(Street, City, State, ZIP)*

Same as No. 9

13. Type of Report & Period Covered

Final

14. Sponsoring Agency Code

15. SUPPLEMENTARY NOTES

16. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)*

This publication summarizes the proceedings of a conference held for the purpose of highlighting the needs and problems of Federal, State and local government in safeguarding individual privacy and protecting confidential data contained in computer systems from loss or misuse. The Conference was held at the National Bureau of Standards on November 19-20, 1973.

The origin of governmental problems is discussed in the context of the public's concern for privacy arising out of computer-based recordkeeping, the diverse legislative actions how being taken to safeguard privacy, the threats to the security of computer-based information systems and the technological problems associated with protecting against such threats. Useful distinctions are drawn between privacy, confidentiality and security to clarify the issues and allocate responsibilities for solving the problem among lawmakers, technologists and management.

Major needs are described. These include the need for cohesive Federal, State and local legislation, technological guidelines and standards for assuring uniform compliance with legislative requirements; management guidelines for identifying and evaluating threats to security; and improved technological mechanisms for controlling access to computer systems and networks. Cost implications of providing security measures are discussed.

17. KEY WORDS *(six to twelve entries; alphabetical order; capitalize only the first letter of the first key word unless a proper name; separated by semicolons)*

Computer systems, privacy and security; confidentiality; privacy; security.

18. AVAILABILITY [xx] Unlimited

[ ] For Official Distribution. Do Not Release to NTIS

[ ] Order From Sup. of Doc., U.S. Government Printing Office Washington, D.C. 20402, SD Cat. No. C13

[ ] Order From National Technical Information Service (NTIS) Springfield, Virginia 22151

19. SECURITY CLASS (THIS REPORT)

UNCLASSIFIED

21. NO. OF PAGES

47

20. SECURITY CLASS (THIS PAGE)

UNCLASSIFIED

22. Price

85 cents

NBS TECHNICAL PUBLICATIONS

PERIODICALS

JOURNAL OF RESEARCH reports National Bureau of Standards research and development in physics, mathematics, and chemistry. Comprehensive scientific papers give complete details of the work, including laboratory data, experimental procedures, and theoretical and mathematical analyses. Illustrated with photographs, drawings, and charts. Includes listings of other NBS papers as issued.

Published in two sections, available separately:

- **Physics and Chemistry (Section A)**

Papers of interest primarily to scientists working in these fields. This section covers a broad range of physical and chemical research, with major emphasis on standards of physical measurement, fundamental constants, and properties of matter. Issued six times a year. Annual subscription: Domestic, $17.00; Foreign, $21.25.

- **Mathematical Sciences (Section B)**

Studies and compilations designed mainly for the mathematician and theoretical physicist. Topics in mathematical statistics, theory of experiment design, numerical analysis, theoretical physics and chemistry, logical design and programming of computers and computer systems. Short numerical tables. Issued quarterly. Annual subscription: Domestic, $9.00; Foreign, $11.25.

DIMENSIONS, NBS

The best single source of information concerning the Bureau's measurement, research, developmental, cooperative, and publication activities, this monthly publication is designed for the layman and also for the industry-oriented individual whose daily work involves intimate contact with science and technology *—for engineers, chemists, physicists, research managers, product-development managers, and company executives.* Annual subscription: Domestic, $6.50; Foreign, $8.25.

NONPERIODICALS

Applied Mathematics Series. Mathematical tables, manuals, and studies.

Building Science Series. Research results, test methods, and performance criteria of building materials, components, systems, and structures.

Handbooks. Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications. Proceedings of NBS conferences, bibliographies, annual reports, wall charts, pamphlets, etc.

Monographs. Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

National Standard Reference Data Series. NSRDS provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated.

Product Standards. Provide requirements for sizes, types, quality, and methods for testing various industrial products. These standards are developed cooperatively with interested Government and industry groups and provide the basis for common understanding of product characteristics for both buyers and sellers. Their use is voluntary.

Technical Notes. This series consists of communications and reports (covering both other-agency and NBS-sponsored work) of limited or transitory interest.

Federal Information Processing Standards Publications. This series is the official publication within the Federal Government for information on standards adopted and promulgated under the Public Law 89–306, and Bureau of the Budget Circular A–86 entitled, Standardization of Data Elements and Codes in Data Systems.

Consumer Information Series. Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

BIBLIOGRAPHIC SUBSCRIPTION SERVICES

The following current-awareness and literature-survey bibliographies are issued periodically by the Bureau:

Cryogenic Data Center Current Awareness Service (Publications and Reports of Interest in Cryogenics). A literature survey issued weekly. Annual subscription: Domestic, $20.00; foreign, $25.00.

Liquefied Natural Gas. A literature survey issued quarterly. Annual subscription: $20.00.

Superconducting Devices and Materials. A literature survey issued quarterly. Annual subscription: $20.00. Send subscription orders and remittances for the preceding bibliographic services to the U.S. Department of Commerce, National Technical Information Service, Springfield, Va. 22151.

Electromagnetic Metrology Current Awareness Service (Abstracts of Selected Articles on Measurement Techniques and Standards of Electromagnetic Quantities from D-C to Millimeter-Wave Frequencies). Issued monthly. Annual subscription: $100.00 (Special rates for multi-subscriptions). Send subscription order and remittance to the Electromagnetic Metrology Information Center, Electromagnetics Division, National Bureau of Standards, Boulder, Colo. 80302.

Order NBS publications (except Bibliographic Subscription Services) from: Superintendent of Documents, Government Printing Office, Washington, D.C. 20402.

U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards
Washington, D.C. 20234

OFFICIAL BUSINESS

Penalty for Private Use, $300

POSTAGE AND FEES PAID
U.S. DEPARTMENT OF COMMERCE
COM-215

U.S.MAIL